A Thieves Identification Scheme for Prepaid Systems in Smart Grids

Zhiyuan Sui(✉), Hengyue Jia, Fu Chen, and Jianming Zhu

Information School, Central University of Finance and Economics, Beijing, China

Abstract. This paper proposes a privacy preserving thieves identification scheme for prepaid Smart Grid systems. Prepaid systems allow consumers to buy credentials from an operation center before consumption. According to the credentials, consumers can use the corresponding amount of electricity. Based on the dynamic k-times anonymous authentication protocol, the scheme can achieve thieves identification and privacy preservation at the same time without the involvement of a trusted authority in the system. Finally, we point out the path of our future work.

Keywords: Smart grid · Anonymity · Privacy · Security

1 Introduction

With the development of public awareness of environmental conservation, more and more renewable energy come to use. However, the renewable energy sources are so volatile that the power companies have to employ the Information and Communication Technologies (ICT) to balance the power production and consumption. The power company aggregates the power usage reports from consumers to calculate the amount of power consumption. The usage reporting device at each customer site is called as smart meter. The operation center and smart meters form the Smart Grid. The invention of Smart Grids is a great plus to the electricity industry. This mechanism can be exploited to improve energy efficiency and infrastructure reliability. However, trustless data, which does not represent the real consumption, may damage the electricity grid infrastructure [1]. At the same time, the billing information is generated by the usage data. Greedy thieves are not willing to send the trustworthy data and pay for their consumption. Hence, it is a serious challenge to resist fake data and detect power thieves in Smart Grids. On the other hand, privacy is another key requirement in Smart Grids. The usage data from the consumer should not result in finding consumers' usage information, which could lead to disclosure of the consumer's living habits or production outputs, and further causes personalized advertisements or intelligence leakage [2].

To solve the security and privacy preservation challenges, power request model was proposed for prepaid card system. The prepaid smart card system

B. Chen and X. Huang (Eds.): AC3 2021, LNICST 386, pp. 175–180, 2021.
https://doi.org/10.1007/978-3-030-80851-8_13

allows consumers buy credentials from the power company in advance. When the consumer needs power in the existing privacy preserving prepaid card system, he just sends the usage plan with his transformed credentials to the operation center. The operation center will send the power back according to the number of credentials [3]. However, credentials may be collision due to large data base. Moreover, the scheme [3] cannot identify thieves.

Taking the requirements of privacy preservation and thieves identification into account, in this paper, we construct a secure and privacy preserving thieves identification scheme in Smart Grids. There are two important virtues: (1) the scheme resists credential collisions; (2) energy thieves can be identified in the prepaid system.

The rest of this paper is organized as follows. Section 2 discusses related work in the prepaid system domain. Section 3 elaborates and explains necessary system models. In Sect. 4, we describe our proposed scheme. Finally, the paper is concluded in Sect. 5.

2 Related Work

To solve the security and privacy preservation challenges, power request models for smart grid systems have been proposed [3]. In such models, consumers receive tokens signed with blind signatures from the power provider and authenticate themselves using blinded tokens. The tokens represent a corresponding denomination of energy cost. Consequently, the power provider knows the total amount of customer energy costs but do not know the details of the usage information. However, this scheme cannot identify power thieves. Dimitriou et al. [4] added a proof to the blind signature. According to the proof, reused tokens from the same consumer can be identified. However, the tokens are generated by the consumers, and token collisions are inevitable. Zhao et al. [5] employed a fully homomorphic encryption algorithm to aggregate smart meters' usage data. Based on the homomorphism of the ciphers, consumers' billing can be calculated without knowing the plaintexts. However, current fully homomorphic encryption algorithms are less efficient. Xue et al. [6] improved the Paillier encryption algorithm. The exponent on the cipher is also additive homomorphism. Therefore, it can also achieve dynamic billing management with less computational cost. Li et al. [7] divided the usage data into multiple parts according to their denominations. In their study, each smart meter holds a corresponding number of key pairs with respect to the divided sets. Therefore, smart meters belonging to different sets should pay their corresponding billings.

Smart Grids cannot ensure improvement in infrastructure reliability without trustworthy information. At the same time, consumers do not wish their energy usage data to be exposed to the operation center. However, existing thieves identification approaches cannot make use of a trade-off between privacy and security. According to prepaid card systems, this paper proposes a privacy-preserving thieves identification scheme without any trusted authority. In this scheme, a thief can be traced if sending a used credential.

3 The Framework

In this section, the assumed network and security requirements in the scheme are described.

3.1 Network Model

Nowadays, in order to improve energy efficiency and infrastructure reliability, a prepaid system is proposed [3]. In the scheme, the system model mainly consists of two entities: the operation center (OC) and the smart meter (SM). The number of smart meters is large enough for each smart meter to cloak its usage behavior. As depicted in Fig. 1, firstly, SMs join the Smart Grid and obtain their commitments from the OC. Secondly, each SM buys credentials from the OC. Thirdly, a SM sends blinded commitments and credentials in an anonymized form when it needs to purchase electricity.

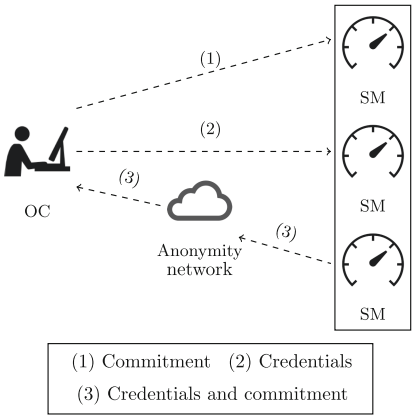

Fig. 1. Network model.

3.2 Security Requirements

The privacy-preserving thieves identification scheme is expected to exhibit the following properties:

1. **Privacy Preservation:** Curious eavesdroppers cannot obtain consumers' usage profiles from the usage reports from smart meters.
2. **Unlinkability:** The adversary cannot link different usage reports from the same smart meter.
3. **Authentication:** The operation center ensures that the usage reports are from legitimate smart meters in the Smart Grid.
4. **Traceability:** Energy thieves can be traced if they attempt to send used credentials.

4 Our Proposed Approach

In this section, a privacy-preserving thieves identification scheme is proposed based on the dynamic k-times anonymous authentication scheme.

4.1 Setup

In the privacy-preserving thieves identification scheme, a concrete region is managed by a single operation center. The operation center runs the setup algorithm on input of the security size κ to obtain a group public key and a secret key as follows:

1. Let p be a prime number of size κ, $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be three cyclic groups of prime order p. Suppose P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, and e is a bilinear map. On input of κ, the bilinear pairing instance generator returns a tuple $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathbb{Z}_p^*, e, P_1, P_2)$.
2. Then, the operation center chooses collision-resistant hash functions $\mathcal{H}_{\mathbb{Z}_p^*} : \{0,1\}^* \to \mathbb{Z}_p^*$ and $\mathcal{H}_{\mathbb{G}^2} : \{0,1\}^* \to (\mathbb{G}_1, \mathbb{G}_1)$, two elements $V, Q \in \mathbb{G}_1$ and $\gamma \in \mathbb{Z}_p^*$, and computes $P_{\text{pub}} = \gamma P$.
3. Finally, the operation center retains its secret key γ, publishes its public key $(P_1, P_2, V, Q, P_{\text{pub}})$, and builds an empty authentication log **LOG** that records the used credentials.

4.2 Joining

The joining protocol is carried out between the operation center and a smart meter. Each household or company is equipped with a smart meter in the Smart Grid system. A secure public key signature scheme, including a signing algorithm **sig** and a verification algorithm **ver**, is selected for a smart meter. In this protocol, the smart meter must reveal its unique identity ID_j to the operation center as follows. Firstly, the smart meter generates a secure parameter $x_j \in \mathbb{Z}_p^*$, computes a request $C_j = x_j P_1$ and generates a signature $\sigma = \mathbf{sig}(C_j \| \text{ID}_j)$. The smart meter sends the signature σ with the request C_j and identity ID_j to the operation center. Upon the receipt, the operation center computes a hash value $f_j = \mathcal{H}_{\mathbb{Z}_p^*}(\text{ID}_j)$, grants the request $S_j = \frac{1}{(f_j+\gamma)}(C_j + Q)$ and replies S_j. Upon receipt, the smart meter confirms that the equation $e(S_j, f_j P_2 + P_{\text{pub}}) = e(x_j P_1 + Q, P_2)$ holds. Finally, the smart meter retains its secret key x_j and publishes its public key (C_j, S_j).

4.3 Power Purchasing

The power-purchasing protocol is carried out between the operation center and a smart meter. Using this protocol, the smart meters buy credentials from the operation center and are granted the right to obtain electricity.

Periodically, the operation center publishes the bound number $k > 0$ and calculates the set of public credentials $\{(t_i, \hat{t}_i) = \mathcal{H}_{\mathbb{G}^2}(i, n_T) \mid 1 \leq i \leq k\}$,

where n_T denotes the timestamp. The public credential $(t_i, \hat{t}_i)$ is called the ith credential base of the operation center. If q smart meters want to buy k units of electricity, represented by k credentials, the smart meters send their identities to the operation center. The operation center calculates $\{f_j = \mathcal{H}_{\mathbb{Z}_p^*}(\mathrm{ID}_j) \mid 1 \leq j \leq q\}$ and $W = \sum_{j=1}^{n}(\gamma + f_j)V$ and $V_j = \frac{1}{\gamma + f_j}W$ for the jth smart meter. The operation center publishes $\{(t_i, \hat{t}_i) \mid 1 \leq i \leq k\}$ and sends V_j to the smart meter ID_j. The smart meter operates a counter μ_j, which is initially set to zero.

4.4 Power Requesting

The power-requesting protocol is run by the operation center and a smart meter to prove knowledge of a smart meter's key x_j and an identity hash value f_j. The smart meter transforms its commitment and credentials, and sends them back to the operation center. Therefore, the operation center cannot locate the source of the public parameters even though the credentials generated by itself.

1. Firstly, the smart meter analyzes the usage data and estimates the amount of energy m. The smart meter increases the counter number by m.
2. If $\mu_j > k$, the smart meter will jump to the power-purchasing algorithm; otherwise, the smart meter sets $\mu_j = \mu_j + m$, chooses m credentials denoted as $(t_1, \hat{t}_1)$, ..., $(t_m, \hat{t}_m)$, and outputs m hash values $\{c_i = \mathcal{H}_{\mathbb{Z}_p^*}(t_i \| \hat{t}_i \| n_T) \mid 1 \leq i \leq m\}$, where n_T denotes the timestamp.
3. After that, the smart meter computes the credentials $\{(\Gamma_i = x_j t_i, \hat{\Gamma}_i = f_j t_i + c_i x_j \hat{t}_i) \mid 1 \leq i \leq m\}$, and generates a proof using the following non-interactive zero-knowledge proof:

$$\left\{ \begin{pmatrix} S_j \\ x_j \\ f_j \\ V_j \end{pmatrix} : \begin{array}{l} e(S_j, f_j P_2 + P_{\mathrm{pub}}) = e(x_j P_1 + Q, P_2) \\ e(V_j, f_j P_2 + P_{\mathrm{pub}}) = e(W, P_2) \\ (\Gamma_i = x_j t_i, \hat{\Gamma}_i = f_j t_i + x_j c_i \hat{t}_i) \end{array} \right\}$$

   The smart meter proves its credentials by sending the proof and transformed credential to the operation center. Please refer to [8] for the proof.
4. After receiving the proof and credential, the operation center checks the validity of the timestamp. If it is valid, the operation center compares the credential $(\Gamma_i, \hat{\Gamma}_i)$ with all corresponding credentials in **LOG**, and checks if it is different to the credentials in **LOG**. Finally, the operation center verifies that the proof does prove knowledge of its identity information.

4.5 Identification

If the operation center validates the signature σ and discovers that a received credential has already been used, it will run the identification algorithm. Suppose there are two credentials (Γ_i, n_T) and (Γ_i', n_T'), where $\Gamma_i = \Gamma_i'$ and $n_T \neq n_T'$. The operation center can confirm that a credential has been used more than once.

Then, the operation center computes $c = \mathcal{H}_{\mathbb{Z}_p^*}(t_i \| \hat{t}_i \| n_T)$, $c' = \mathcal{H}_{\mathbb{Z}_p^*}(t_i \| \hat{t}_i \| n'_T)$ and $\beta = \frac{c'\hat{\Gamma}_i - c\hat{\Gamma}'_i}{c-c'}$, searches for the ID_j which satisfies $\beta = \mathcal{H}_{\mathbb{Z}_p^*}(\mathrm{ID}_j)t_i$.

The public keys $\{(t_i, \hat{t}_i) \mid 1 \leq i \leq k\}$ are produced by a collision-resistant function, making the transformed credentials $\{(\Gamma_i, \hat{\Gamma}_i) \mid 1 \leq i \leq k\}$ also resistant to collisions. Therefore, malicious smart meters cannot deny their misbehavior.

5 Conclusion

Energy theft occurs frequently in Smart Grids due to its large amount of consumers. In order to defend against energy theft under prepaid smart grid systems, this paper proposes a scheme to achieve identification of thieves without a trusted party. Only an operation center and smart meters are required in the scheme. The operation center checks the smart meters' commitments and corresponding credentials. Therefore, the credentials are resistant to collisions. Great computational capacity is required for operation centers. For the future work, we will study possible ways and improve k-times anonymous authentication scheme to reduce the computational cost during power request procedures.

Acknowledgement. This work is supported by Funds of the National Natural Science Foundation of China (U201509214), (61672104), (62072487) and (61906220).

References

1. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: threats and potential solutions. Comput. Netw. **169**(14), 107094 (2020)
2. Ferraga, M.A., Maglarasc, L.A., Janickec, H., Jiang, J.: A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustain. Cities Soc. **38**, 806–835 (2018)
3. Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.-K.: Privacy-preserving advance power reservation. IEEE Commun. Mag. **50**(8), 18–23 (2012)
4. Dimitriou, T., Karame, G.: Enabling anonymous authorization and rewarding in the smart grid. IEEE Trans. Dependable Secure Comput. **14**(5), 565–572 (2017)
5. Zhao, S., Li, F., Li, H., Lu, R., Ren, S.: Smart and practical privacy-preserving data aggregation for fog-based smart grids. IEEE Trans. Inf. Forensics Secur. **16**, 521–536 (2021)
6. Xue, K., et al.: PPSO: a privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid. IEEE Internet Thins J. **6**(2), 2486–2496 (2019)
7. Li, S., Zhang, X., Xue, K., Zhou, L., Yue, H.: Privacy-preserving prepayment based power request and trading in smart grid. Chin. Commun. **15**(4), 24–37 (2018)
8. Nguyen, L., Safavi-Naini, R.: Dynamic k-times anonymous authentication. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 318–333. Springer, Heidelberg (2005). https://doi.org/10.1007/11496137_22